UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/996,283	11/27/2001	Thomas J. Parenty	020906-000120US	4043

23493 7590 12/30/2005

SUGHRUE MION, PLLC
401 Castro Street, Ste 220
Mountain View, CA 94041-2007

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/996,283	PARENTY, THOMAS J.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 November 2001*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 09/23/2005.

2. Claims 1-23 are pending.

Response to Arguments

3. In regarding to the Double Patenting rejection dated 03/23/2005, the copending application 09/735,876 went abandoned on February 2nd, 2005. Therefore, the Double Patenting rejection is withdrawn.

4. Applicant's arguments filed 09/23/2005 have been fully considered but they are not persuasive.

5. As per argument on page 11, Applicant argues that Sasaki does not discloses the "key management component". In light of the claim language, Sasaki clearly discloses the "key management component", which can either the transmitter or the receiver. Sasaki discloses clearly 13 embodiments in the patent. The functionalities of the "key management component" in the claimed invention can be done in either the transmitter or receiver. However, in the Sixth Embodiment of the patent in Col 14 lines 1-40, Sasaki discloses the steps that the receiver ("key management component") transmits the objection encryption component to the transmitter to generate the symmetrical key (common key), public key of the

receiver ("Key management component"), the objection encryption component to encrypt the text using the symmetric key (common key), and the identifier I or the association between the encrypted symmetric key and the cipher text object (Col 14 lines 20-26). Then the transmitter (active agent) transmits the ciphertext, the identifier I, and a first enciphered common key I (Col 14 lines 27-32). Therefore, it is clearly that Sasaki discloses the "key management component" (argued on page 11) and the public/private key pairs used to encrypt the generated symmetric key (argued on page 12 3rd paragraph).

6. Therefore, Sasaki clearly discloses the claims 1-23.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "key management component" is the only element in the invention that performs the operation of public/private key generation (see step 500, Figs 4&5)", and ""the presently claimed invention only needs to create one public/private key pair, which further reduces administrative overhead and security vulnerabilities when compared to the cited reference".) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-3, 5, 7, 9-12, 14, 16, and 18-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Sasaki et al, US Patent No. 6351536, hereinafter "Sasaki".

10. As per claim 1:

Sasaki teaches "A method of encrypting an object, comprising the steps of: a first active agent initiating the first key management component generating a first key management component public key/first key management component private key pair (Col 10 lines 14-17); loading an object encryption component; loading an object decryption component; creating a correlation table; a second active agent transmitting an encrypt object request to the first key management component (Col 3 lines 22-26, Col 9 lines 25-31); the first key management component transmitting an object encryption component to the second active agent computing platform over a secure channel (Col 9 lines 40-44); the first key management component transmitting the first key

management component public key to the active agent computing platform over a secure channel (Col 9 lines 40-44); the object encryption component generating a symmetric key (Col 10 lines 5-9); the object encryption component encrypting a clear text object with the symmetric key (Col 9 lines 32-34); the object encryption component encrypting the symmetric key with the first key management component public key (Col 7 lines 50-59); the object encryption component creating an association between the encrypted symmetric key and the cipher text object (Col 2 lines 14-17 and Col 7 lines 50-59); the object encryption component transmitting the encrypted symmetric key to the first key management component or to a second key management component having the first key management component private key (Col 7 lines 12-35) ; the object encryption component transmitting the association to the key management component having received the encrypted symmetric key (Col 7 lines 12-35); and, the key management component having received the association entering the association into the correlation table (Col 17 lines 18-23).

11. As per claim 3:

Sasaki teaches "The method of claim 1, wherein the first key management component public key/first key management component private key pair is generated using an encryption algorithm selected from the group consisting of ECC and RSA (Col 10 lines 14-17).

12. As per claims 5 and 14:

Sasaki teaches "The method of claims 1 and 14, wherein the object encryption/decryption component is installed on a browser" in (Col 2 line 64 thru Col 3 line 4).

13. As per claims 7 and 16:

Sasaki teaches "The method of claims 5 and 14, wherein the object encryption component is implemented as a Java.RTM. applet" in (Col 9 lines 25-31).

14. As per claims 9 and 18:

Sasaki teaches "The method of claims 1 and 18, wherein the object encryption component is comprised of a symmetric encryption algorithm selected from the group consisting of IDEA, DES, Blowfish, RC4, RC2, SAFER, and AES" in (Col 7 lines 57-59).

15. As per claim 10:

Sasaki teaches "A method of decrypting an object, comprising the steps of: an active agent transmitting a decrypt object request to the key management component (Col 14 lines 20-26); the key management component retrieving a cipher text object symmetric key from a correlation table (Col 8 lines 35-39); the key management component decrypting cipher text object symmetric key with the key management component private key (Col 7 line 66 thru Col 8 line 3); the key management component

transmitting the object decryption component to the active agent computing platform over a secure channel (Col 14 lines 20-26); the key management component transmitting the cipher text object symmetric key to the active agent computing platform over a secure channel (Col 13 lines 58-67 and Col 14 lines 20-26); and the object decryption component decrypting the cipher text object with the cipher text object symmetric key (Col 13 lines 64-67).

16. As per claims 2 and 19:

Sasaki teaches "A method of encrypting an object, comprising: under control of a first encryption server system, generating a public/private key pair for an encryption server system (Col 10 lines 14-17); under control of a client system, requesting an encryption program from an encryption server system (Col 3 lines 22-26, and Col 9 lines 25-31); requesting a server public key from an encryption server system (Col 3 lines 22-26, and Col 9 lines 25-31); under the control of an encryption server system, transmitting an encryption program to a client system over a secure channel (Col 9 lines 40-44); transmitting a server public key to a client system over a secure channel (Col 9 lines 40-44); under control of a client system, receiving an encryption program from an encryption server system over a secure channel (Col 9 lines 40-44); receiving a server public key from an encryption server system over a secure channel (Col 9 lines 40-44); installing an encryption program on a client system; running an encryption program on a client system to generate a symmetric key (Col 10 lines 5-9); encrypting a clear text object with a symmetric key, thereby creating a cipher text object (Col 9 lines 32-34);

creating a relationship between a cipher text object and a symmetric key; encrypting symmetric key with an encryption server public key, thereby creating an encrypted symmetric key (Col 7 lines 50-59); creating a relationship between a cipher text object and an encrypted symmetric key (Col 2 lines 14-17 and Col 7 lines 50-59); transmitting a cipher text object to an encryption server system; transmitting an encrypted symmetric key to an encryption server system; transmitting the relationship between a cipher text object and an encrypted symmetric key to an encryption server system (Col 7 lines 57-59 and Col 7 lines 12-35); under the control of an encryption server system, storing a cipher text object in a storage medium; storing an encrypted symmetric key in a storage medium (Col 7 lines 25-29); and storing the relationship between a cipher text object and an encrypted symmetric key in a storage medium (Col 17 lines 18-23).

17. As per claims 11-12, and 21:

Sasaki teaches "An encryption system for transparent key management object encryption, comprising: an encryption server system and a client system; an encryption server system, using the first entry in a correlation table to retrieve an encrypted symmetric key (Col 8 lines 35-39); decrypting a symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key (Col 7 line 66 thru Col 8 line 3); inserting a symmetric key into a decryption program; sending a decryption program to a client system over a secure channel (Col 13 lines 58-67 and Col 14 lines 20-26); sending a cipher text object to a client system (Col 13 lines 55-57); under control of a client system, requesting a cipher text object from a server (Col 13

lines 55-57); under control of an encryption server system, installing a decryption program on a client system (Col 14 lines 20-31); and, decrypting a cipher text object using a decryption program, thereby creating a clear text object (Col 13 lines 64-67).

18. As per claim 22:

Sasaki teaches " An encryption system for transparent key management object encryption, comprising: an encryption server system and a client system; under control of an encryption server system, generating a symmetric key (Col 13 lines 39-43); encrypting a clear text object with a symmetric key, thereby creating a cipher text object (Col 9 lines 32-34); inserting a symmetric key into a decryption program; sending a decryption program to a client system over a secure channel (Col 13 lines 58-67 and Col 14 lines 20-26); sending a cipher text object to a client system (Col 13 lines 55-57); under control of a client system, requesting a clear text object from a server (Col 13 lines 55-57); installing a decryption program on a client system (Col 14 lines 20-31); and, decrypting a cipher text object using a decryption program, thereby creating a clear text object (Col 13 lines 64-67).

19. As per claims 20 and 23:

Sasaki teaches "An encryption system for transparent key management object encryption, comprising: an encryption server system and a client system; an encryption server system, generating a public/private key pair for an encryption server system (Col 13 lines 39-43); transmitting an encryption program to a client system over a secure

channel (Col 9 lines 40-44); transmitting a server public key to a client system over a secure channel (Col 9 lines 40-44); storing a cipher text object in a storage medium; storing an encrypted symmetric key in a storage medium; storing the relationship created between a cipher text object and an encrypted symmetric key in a storage medium (Col 7 lines 25-29); using the first entry in a correlation table to retrieve an encrypted symmetric key (Col 8 lines 35-39); decrypting a symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key (Col 7 line 66 thru Col 8 line 3); inserting an encrypted symmetric key into a decryption program; sending a decryption program to a client system over a secure channel (Col 13 lines 58-67 and Col 14 lines 20-26); sending a cipher text object to a client system (Col 13 lines 55-57); decrypting an encrypted symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key (Col 7 line 66 thru Col 8 line 3); sending a cipher text object to a client system (Col 13 lines 55-57); generating a symmetric key (Col 13 lines 39-43); encrypting a clear text object with a symmetric key, thereby creating a cipher text object (Col 13 lines 47-49); a client system, requesting an encryption program from an encryption server system (Col 3 lines 22-26 and Col 9 lines 25-31); requesting a server public key from an encryption server system (Col 10 lines 14-17); receiving an encryption program from encryption server system over a secure connection (Col 9 lines 40-44); receiving a server public key from an encryption server system over a secure channel Col 9 lines 40-44); installing an encryption program on a client system (Col 10 lines 5-9); running an encryption program on a client system to generate a symmetric key (Col 10 lines 5-9); encrypting a clear text object with a

symmetric key, thereby creating a cipher text object (Col 9 lines 32-34); creating a relationship between a cipher text object and a symmetric key (Col 2 lines 14-17); encrypting symmetric key with an encryption server public key, thereby creating an encrypted symmetric key (Col 7 lines 50-59); creating a relationship between a cipher text object and an encrypted symmetric key (Col 2 lines 14-17; col 7 lines 50-59); transmitting an object encrypted with a symmetric key from a client system to an encryption server system (Col 7 lines 57-59); transmitting a symmetric key encrypted with a server public key from a client system to a encryption server system (Col 7 lines 57-59); transmitting the relationship between a cipher text object and an encrypted symmetric key to an encryption server system (Col 9 lines 32-35 and Col 7 lines 57-59); requesting a cipher text object from a server (Col 13 lines 55-57); installing a decryption program on a client system (Col 14 lines 20-31); and, decrypting a cipher text object using a decryption program, thereby creating a clear text object; and, requesting a clear text object from a server (Col 13 lines 64-67).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 4, 6, 8, 13, 15, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasaki.

22. As per claims 4 and 13:

Sasaki teaches "The method of claims 1 and 10". However, Sasaki is silent on "the secure channel is an SSL channel". Nevertheless, Sasaki teaches an encrypted communication between the client's browser and the server in (Col 9 lines 40-44). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art that the encrypted communication can be interpreted as SSL communication. It is well know that the encrypted communication between the client's browser and the server is provided by the SSL protocol.

23. As per claims 6 and 15:

Sasaki teaches "The method of claims 5 and 14 and a web browser" in (Col 3 lines 3-25). However, Sasaki is silent on "wherein the browser is the Internet Explorer^{TM}. or the Navigator.^{RTM}". Nevetheless, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the Internet Explore or the Navigator is well know to be the most popular web browser.

24. As per claims 8 and 17:

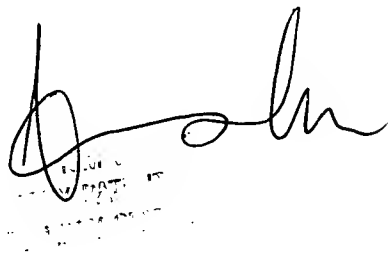
Sasaki teaches "The method of claims 5 and 14 wherein the browser is the Internet Explorer.TM. and the object encryption component is implemented". However, Sasaki is silent on " wherein the browser is the Internet Explorer.TM. and the object encryption component is implemented *as an Active X.TM. control*". Nevertheless, Sasaki teaches

of implementing the Java encryption applet in (Col 9 lines 25-31). Therefore, it would have obvious at the time of the invention was made for one having ordinary skill in the art that the Java encryption applet is well know to be an Active X.™ control.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Linh LD Son
Examiner
Art Unit 2135